Specification of Interfaces for Automotive Software Engineering

lero THE IRISH SOFTWARE ENGINEERING RESEARCH CENTRE

University of Limerick Ollscoil Luimnigh

Pat McElligott

Supervised by	Tony Cahill, Steffen Thiel
Research Area	SPL
Project Title	Reliability and Safety of Embedded Automotive Software

Research Purpose: To Realise a Clearer and More Concise Approach to Specification of Interfaces for Automotive Software Engineering

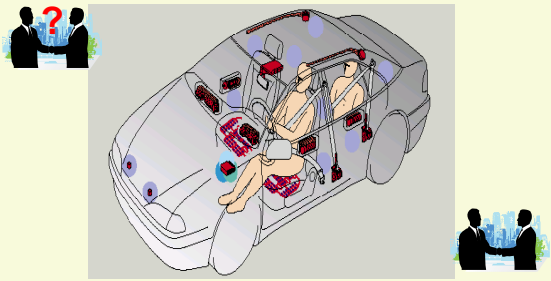

Fig 1 Airbag Control System

- Automotive contracts hinge on clarity and conciseness of
  - Software functional and non-functional interface specification
  - Emerging standards such as AUTOSAR are based on UML2
  - UML2 semantics is textual and informal
  - Emerging Standards do not cater for non-functional aspects

Proposal: Use Trace Function Method (Parnas 2006) and Temporal Logic (Pnueli '77, Gabbay '80, Pneuli '81, Clark 1981) To Realise Clearer and More Concise Interface Specification

- TFM uses a predicate logic augmented for partial functions
  - avoids contradiction in traditional analysis
  - obviates elimination of undefined terms needed in traditional logic
- Intended to be concise/ readable without compromising logical rigor
- TMF treats module as a black-box, identifying
  - programs and data structures accessible from outside the module
  - all externally-visible actions of the module
- Temporal logic used to specify reactive system behaviour over time
  - succinct and natural expression of temporal requirements

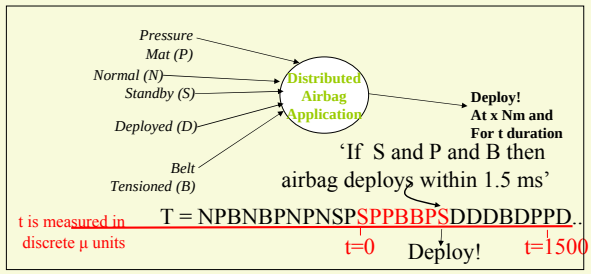

Fig 2 Airbag Functionality Trace Example

1. Initially the trace (T) shows that the vehicle status is normal (N)
2. Seat occupant and belt usage readings are received (P & B)
3. Then a crash is detected and the status changes to Standby (S)
4. Occupant is adult (P) and seat belt in use (B) and Standby
5. Output deployment signal for a specific force and duration within 1.5 ms of vehicle status changing to Standby
6. Vehicle status changes to Deployed (D), P & B readings continue

Latest Results: A Temporal Logic Enhanced Tabular Expression

Eventually$_{<=1500\mu s}$	**Standby**	**SeatBeltUsed**	**Child**	Deploy at (x / 2) Nm for 2t μs	1
			Adult	Deploy at x Nm for t μs	2
			Empty		3
		⌐**SeatBeltUsed**			
	⌐**Standby**				
Eventually$_{>1500\mu s}$	**Standby**	**SeatBeltUsed**	**Child**	Development Diagnostic	4
			Adult		
			Empty		
		⌐**SeatBeltUsed**			
	⌐**Standby**				

Fig 3 Airbag Control System Temporal Logid Enhanced Tabular Expression

1. Eventually within 1500μs, it is detected that, the vehicle is in standby, the seatbelt is in use and a child occupies the seat. In this case, the airbag is deployed at half of force x and twice duration t.
2. Eventually within 1500μs, it is detected that, the vehicle is in standby, the seatbelt is in use and an adult occupies the seat. In this case, the airbag is deployed at force x and duration t.
3. Eventually within 1500μs, it is detected that, the vehicle is in standby, but the seatbelt is in not use. In this case, the airbag is not deployed.
4. Eventually within 1501+μs, it is detected that, the vehicle is in standby, the seatbelt is in use and a child occupies the seat. In this case, a development diagnostic is logged.

Results To Date

- Conference Paper on Formal Methods and Automotive Software
  - McElligott, P., A. Mjeda, and S. Thiel, *Can Formal Methods Make Automotive Business Sense?*, in *SAE World Congress*. 2008, SAE: Detroit, U.S.A.
- Co-authored report on AUTOSAR for the European Space Agency
- In-depth analysis of TFM and other trace based methods
- In-depth analysis of logics and models of real time

Next Steps

- Examine TMF in light of the Parnas claim: "Time … often considered special in some inexplicable way, also easily considered as global variable and require no special treatment"
- Currently working on mix of timing requirements, such as periodic events, jitter-free events, to see how TMF expresses these and how a combination of Temporal Logic Enhanced Tabular Expressions would express them
- Demonstrate how UML and AUTOSAR can be made clearer and more concise using Temporal Logic Enhanced Tabular Expressions
- Engagement with industry partner currently under discussion for purposes of validating the method

NDP National Development Plan

sfi science foundation ireland